DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

ASSISTANT SECRETARY

APR 14 1980

MEMORANDUM FOR: Mr. H. Stuart Knight
Director
U. S. Secret Service

FROM: Richard J. Davis
Assistant Secretary
(Enforcement and Operations)

SUBJECT: Audio Countermeasures Procedures

Attached are the procedures for the Conduct of United States Secret Service Technical Surveillance Countermeasures that have been approved by the Attorney General and Secretary Miller pursuant to section 1-1004 of Executive Order No. 12036 and section 105(f) of the Foreign Intelligence Surveillance Act of 1978. Also attached is Treasury Order No. 105-3 by which the Secretary has delegated his responsibilities and authorities under the procedures to me.

While these procedures became effective on March 31, 1980, I recognize that the Secret Service has been operating under interim guidance previously approved by me and sent to the Justice Department.

Please have your staff refer any questions on interpretation to Mr. Robert McBrien.

Attachments

PROCEDURES FOR THE CONDUCT OF UNITED STATES SECRET SERVICE TECHNICAL SURVEILLANCE COUNTERMEASURES

1. These procedures are adopted in accordance with section 1-1004 of Executive Order No. 12036 and Section 105(f) of the Foreign Intelligence Surveillance Act of 1978.

2. Pursuant to Section 105(f)(2) of the Foreign Intelligence Act of 1978 and the authority vested in the Secretary of the Treasury by section 1-1004 of Executive Order No. 12036, the United States Secret Service is authorized to --

(a) Conduct activities to determine the existence and capability of surveillance equipment being used against the President, Vice President and areas located within the White House-Old Executive Office Building Complex, and

(b) Provide technical countermeasures security for such other Secret Service protectees and other United States officials as may be authorized by --

(1) The Secretary of the Treasury, or

(2) The President.

3. For the purposes of these procedures, the term "technical countermeasures" shall include those techniques utilized to detect or prevent any type of information, electronic or otherwise, from unauthorized transmission.

4. The provision of technical countermeasures security for any protectee, official or area not specified in paragraph 2(a) or authorized by the President shall be at the discretion of the Secretary or his designee. In making a determination, the

Secretary or his designee may require the submission of a written request explaining both the rationale and necessity for such technical countermeasures, describing the area to be inspected, the frequency of inspection; and providing such other information as he deems relevant. The Secretary or his designee shall be advised by the Secret Service of any technical countermeasures security provided at the direction of the President.

5. Continuing technical countermeasures security requested pursuant to Section 4 will be provided by the Secret Service only upon the condition that the requesting entity prior to the institution of such support places and, thereafter, maintains appropriate physical security on all areas where such inspections are provided. The Special Agent in Charge, Technical Security Division (SAIC-TSD), United States Secret Service, is designated the approving authority for an area's physical security standards prior to a technical countermeasures inspection. The authorized user agency may institute physical security controls stricter than those designated by the SAIC-TSD, provided they are approved in advance by the SAIC-TSD. In the event that a user agency declines to implement any recommendation of a technical security nature made by the SAIC-TSD, the Director of the Secret Service will refer the matter to the Secretary or his designee for consideration before the final determination.

6. In any situation in which technical countermeasures are supplied for the security of United States officials not otherwise

authorized Secret Service protection, such technical countermeasures will be supplied on a reimbursable basis pursuant to Section 686 of Title 31, United States Code.

7. The use of technical countermeasures, not targeted against the communications of any particular person or persons, to determine the existence and capability of electronic surveillance equipment being used unlawfully in the United States is permitted if:

(a) Such measures do not result in the acquisition of the contents of communications without the consent of at least one party to the communications and therefore do not amount to electronic surveillance; or

(b) Where it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance, so long as

(i) Any electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(ii) Any information acquired by such surveillance is used only to protect information from unauthorized surveillance, according to paragraph 8 below, or is disseminated only to appropriate law enforcement agencies to enforce Chapter 119 of Title 18 or Section 605 of Title 47.

8. Information, other than communications or portions thereof, acquired by such surveillance may be disseminated to persons within the United States Secret Service and the Office of the Secretary, Department of the Treasury, who require such information in the performance of their duties. Communications or portions thereof acquired by such surveillance may be disseminated within the United

States Secret Service and the Office of the Secretary, Department of the Treasury, only to protect information from unauthorized surveillance. Neither such communications and portions thereof nor other information concerning any technical penetration or hazard involving officials or facilities specified in paragraph 2(a) may be disseminated further unless such dissemination is both consistent with paragraph 7(b)(ii) and is essential to locate or identify the source of such penetration or hazard, or unless the President has specifically approved further dissemination consistent with paragraph 7(b)(ii). Any essential dissemination will be reported immediately to the Secretary or his designee. When officials or facilities under paragraph 2(b) are involved, the procedural guidelines of the Technical Surveillance Countermeasures Subcommittee will be followed.

9. The use of technical countermeasures, not targeted against the communications of any particular person or persons, to train personnel in the use of audio countermeasures equipment is permitted if:

(a) Such measures do not result in the acquisition of the contents of communications without the consent of at least one party to the communications and therefore do not amount to electronic surveillance; or

(b) Where it is not reasonable to obtain consent of persons incidentally subjected to the surveillance so long as:

(i) Such training is limited in extent and duration to that necessary to train the personnel; and

(ii) All contents of any communications acquired are

destroyed as soon as reasonably possible and are not retained or disseminated for any purpose; or

(c) Such training is conducted in the course of authorized technical countermeasures.

10. These procedures shall become effective immediately upon their approval by the Attorney General.

17 March 1980
Date

Secretary of the Treasury

I approve the foregoing procedures in accordance with Section 1-1004 of Executive Order 12036. In my opinion, these procedures are lawful and comply with the provisions of Executive Order 12036 and the Foreign Intelligence Surveillance Act of 1978.

3/31/80
Date

Attorney General